

THUE EQUATIONS AND LATTICES

JEFFREY LIN THUNDER

ABSTRACT. We consider Diophantine equations of the kind $|F(x, y)| = m$, where $F(X, Y) \in \mathbb{Z}[X, Y]$ is a homogeneous polynomial of degree $d \geq 3$ that has non-zero discriminant and m is a positive integer. We prove results that simplify those of Stewart and provide heuristics for a conjecture of Stewart.

INTRODUCTION

Suppose $F(X, Y) \in \mathbb{Z}[X, Y]$ is a homogeneous polynomial of degree $d \geq 3$ that has non-zero discriminant and m is a positive integer. In this paper we are concerned with the number of primitive, i.e., x and y are relatively prime, solutions $(x, y) \in \mathbb{Z}^2$ to the Thue equation

$$|F(x, y)| = m. \tag{1}$$

Thue in [8] famously showed that the number of such solutions is necessarily finite under the hypothesis that F is irreducible over \mathbb{Q} . In fact, his method enabled one to derive an upper bound on the number of such solutions; such an upper bound would depend on m and the polynomial F . Indeed, Lewis and Mahler in [4] provided just such a bound. Their bound was an explicit function of m , d and the height of F . Previous to the result of Lewis and Mahler, Siegel had made the conjecture that an upper bound could be obtained that was independent of the particular coefficients of the polynomial F . Evertse proved this conjecture in his doctoral thesis (see [3]). A few years later Bombieri and Schmidt [2] improved markedly on Evertse's bound, showing that the number of primitive solutions to (1) is no more than some fixed (absolute) constant multiple of $d^{1+\omega(m)}$, where $\omega(m)$ denotes the number of distinct prime factors of m , as usual. Later Schmidt posited (see [6, chap. 3, Conjecture]) that the number of primitive solutions to (1) should be bounded above by some multiple (possibly depending on F) of a power of $\log m$ when $m > 1$.

Two years after the publication of Bombieri and Schmidt's result, Stewart [7] provided a bound that was often (depending on the prime factorization of the parameter m) much stronger than the bound of Bombieri and Schmidt. Stewart's main result was somewhat involved and complicated to state, but one can easily state the following consequence. In what follows, $D(F)$ denotes the discriminant of the form F .

Theorem (Stewart). *Suppose $F(X, Y) \in \mathbb{Z}[X, Y]$ is a homogeneous polynomial of degree $d \geq 3$ with non-zero discriminant and content 1. Let $\epsilon > 0$. Suppose m is a positive integer and m' is a divisor of m relatively prime to $D(F)$ that satisfies $(m')^{1+\epsilon} \geq m^{(2/d)+\epsilon}/|D(F)|^{1/d(d-1)}$. Then the number of primitive solutions to (1) is at most*

$$\left(5600d + \frac{700}{\epsilon}\right) d^{\omega(m')}.$$

The constants 5600 and 700 here carry no particular importance beyond specificity. The major improvement over the result of Bombieri and Schmidt is that the quantity $\omega(m')$ is possibly much smaller than $\omega(m)$. In the same paper, Stewart explicitly constructed forms of various degrees to show lower bounds for the number of primitive solutions to (1). In so doing, he was lead to the following.

Conjecture (Stewart). *There is an absolute constant c_0 such that, for all forms F as in the theorem above, there is a positive bound C (depending on F) such that (1) has at most c_0 primitive solutions for all $m \geq C$.*

In this paper we will obtain results which simplify and strengthen Stewart's. Perhaps as important is that our method has the added benefit of providing good heuristics for the conjecture above. In order to state our main results, we introduce a bit more notation.

Denote the set of places of \mathbb{Q} by $M(\mathbb{Q})$. For any $v \in M(\mathbb{Q})$ we let $|\cdot|_v$ denote the usual v -adic absolute value on \mathbb{Q} and \mathbb{Q}_v denote the topological completion of \mathbb{Q} with respect to this absolute value, though we will continue to use $|\cdot|$ for the usual Euclidean absolute value. We fix algebraic closures $\overline{\mathbb{Q}_v}$ for each of these and assume that our original absolute values on \mathbb{Q} are extended to the $\overline{\mathbb{Q}_v}$'s. As usual, we identify the finite places with positive primes.

Any form $F(X, Y) \in \mathbb{Q}[X, Y]$ factors completely into a product of linear forms over some splitting field:

$$F(X, Y) = \prod_{i=1}^d L_i(X, Y).$$

This splitting field may be embedded into any $\overline{\mathbb{Q}_v}$; we abuse notation somewhat and write the above for the factorization of F over $\overline{\mathbb{Q}_v}$ for all places $v \in M(\mathbb{Q})$. These linear factors are only unique up to a scalar multiple, of course. We say a linear factor $L_i(X, Y)$ is defined over \mathbb{Q}_v if all possible quotients of coefficients are in \mathbb{Q}_v . For any form $F(X, Y) \in \mathbb{Z}[X, Y]$ and place $v \in M(\mathbb{Q})$, set $c_F(v)$ to be the number of linear factors that are defined over \mathbb{Q}_v . For any integer $m > 1$ set

$$c_F(m) = \prod_{\substack{p|m \\ p \text{ prime}}} c_F(p).$$

Theorem 1. *Let $F(X, Y) \in \mathbb{Z}[X, Y]$ be a homogeneous polynomial of degree $d \geq 2$ with non-zero discriminant and content 1 and suppose m is a positive integer with $|m|_p < |D(F)|_p$ for all primes $p|m$. Then the primitive $(x, y) \in \mathbb{Z}^2$ with $m|F(x, y)$ are contained in $c_F(m)$ sublattices of \mathbb{Z}^2 of determinant m .*

In particular, there are no solutions to (1) if $c_F(m) = 0$. In other words, $c_F(m) = 0$ implies that there is some local obstruction to solving (1).

Given a sublattice $\Lambda \subseteq \mathbb{Z}^2$ of relatively large determinant, we can provide an upper bound not just on the number of primitive solutions to (1), but even to the related inequality

$$|F(x, y)| \leq m. \tag{1'}$$

Theorem 2. *Let $F(X, Y) \in \mathbb{Z}[X, Y]$ be a homogeneous polynomial of degree $d \geq 3$ with non-zero discriminant and content 1. Suppose m is a positive integer and $\Lambda \subseteq \mathbb{Z}^2$ is a sublattice with $\det(\Lambda) = Am^{2/d}/|D(F)|^{1/d(d-1)}$ for some $A > 0$. If $A \geq 5^4$, then the number of primitive lattice points $(x, y) \in \Lambda$ that are solutions to (1') is less than*

$$2 + 2d \left(11 + \frac{31}{\log(d-1)} + \frac{\log\left(\frac{2 \log m}{d \log A} + 2\right)}{\log(d-1)} \right).$$

If $A < 5^4$, then the number of solutions is less than

$$\frac{2 \cdot 5^4}{A} \left(2 + 2d \left(11 + \frac{31}{\log(d-1)} + \frac{\log\left(\frac{\log m}{2d \log 5} + 2\right)}{\log(d-1)} \right) \right).$$

Corollary. *Let $F(X, Y) \in \mathbb{Z}[X, Y]$ be a homogeneous polynomial of degree $d \geq 3$ with non-zero discriminant and content 1. Suppose m is a positive integer and m' is a divisor of m relatively prime to $D(F)$ that satisfies $m' = Am^{2/d}/|D(F)|^{1/d(d-1)}$ for some $A \geq 1$. Then the number of primitive solutions $(x, y) \in \mathbb{Z}^2$ to (1') with $m'|F(x, y)$ is less than*

$$2500d \left(43 + \frac{\log(2 + \log m / (1 + \log A))}{\log(d-1)} \right) c_F(m').$$

Proof. One readily checks that for $d \geq 3$, $(d/2) \log A \geq 1 + \log A$ if $A \geq 5^4$ and $2d \log 5 \geq 1 + \log A$ if $1 \leq A < 5^4$. The rest follows from Theorems 1 and 2.

Comparing the Corollary with the result of Stewart above, our constants are in the same ballpark even though we are estimating more than just the solutions to (1). Moreover, we can easily replace the 2500 with 2 once $A \geq 5^4$. Our real improvement is replacing Stewart's $d^{\omega(m')}$ term with $c_F(m')$. Clearly $c_F(m') \leq d^{\omega(m')}$ always, but will typically be much smaller. Also, the estimate in Stewart's result tends to infinity as the divisor m' approaches $m^{2/d}/|D(F)|^{1/d(d-1)}$, whereas our estimate is bounded above by a constant multiple of $c_F(m')d \log \log m / \log(d-1)$.

Again, the main novelty of our approach is the lattices; primitive solutions to our Thue equation (1) are elements of certain sublattices of \mathbb{Z}^2 . One may view Theorem 2 as attempting to limit the number $c_F(m')$ of sublattices considered by allowing the divisor m' to be small, yet still allowing for a “good” upper bound for the number of solutions (at least a result as strong as Schmidt's conjecture above, say). Another approach is to take m' as large as possible and see that there are very few solutions to (1') in the associated lattices. This approach can be used to give good heuristics for Stewart's conjecture above. We consider this approach now.

For a given form $F(X, Y) \in \mathbb{Z}[X, Y]$ with non-zero discriminant and positive integer m , we set $m(F)$ to be the largest divisor m' of m with $|m'|_p < |D(F)|_p$ for all primes $p|m'$. Thus, $m(F)$ is the largest divisor of m satisfying the hypotheses of Theorem 1. Clearly any solution (x, y) to (1) satisfies $m(F)|F(x, y)$. For any form F we write \mathbf{F} for the coefficient vector. Given an $F(X, Y)$ with its factorization into linear forms as above and an $\epsilon > 0$, we say a non-zero $(x, y) \in \mathbb{Z}^2$ is ϵ -exceptional if

$$\frac{|L_i(x, y)L_j(x, y)|}{|\det(\mathbf{L}_i^{tr}, \mathbf{L}_j^{tr})|} \leq \frac{1}{\|(x, y)\|^\epsilon}$$

for some indices $i \neq j$, where \mathbf{L}^{tr} denotes the transpose of \mathbf{L} and $\|\cdot\|$ denotes the usual Euclidean norm on \mathbb{C}^2 . In other words, the ϵ -exceptional points are the points dealt with by Roth's theorem (or the Subspace theorem the way we have formulated things here). As is well-known, the number of such exceptional points is bounded above by an explicit function of ϵ and the degree d of F , thus justifying the “exceptional” moniker.

Theorem 3. *Let $F(X, Y) \in \mathbb{Z}[X, Y]$ be a homogeneous polynomial of degree $d \geq 5$ with non-zero discriminant and content 1. For any positive $\epsilon < d - 4$ there is a positive $c(F, \epsilon)$ depending only on F and ϵ such that if $m \geq c(F, \epsilon)$ and Λ is a sublattice of \mathbb{Z}^2 with determinant $m(F)$, then there is at most one pair of primitive solutions $\pm(x, y) \in \Lambda$ to (1') that is not $(d - 4 - \epsilon)$ -exceptional. Further, any such primitive solution must satisfy $\|(x, y)\| < m(F)^{(1/2) - (\epsilon/3(2+\epsilon))}$.*

A major point here is that for m large enough, any primitive solution to (1) that isn't exceptional in the sense of Thue-Siegel-Roth is a non-zero lattice point of length much less than $\sqrt{\det(\Lambda)}$. But now lattices with such a point are exceptional in that their first successive minima (in the sense of Minkowski) is smaller than typical.

Theorem 4. *Let $\delta > 0$. The proportion of sublattices $\Lambda \subseteq \mathbb{Z}^2$ of determinant m with a primitive $(x, y) \in \Lambda$ satisfying $\|(x, y)\| \leq m^{(1/2) - \delta}$ is $O(m^{-2\delta})$ as $m \rightarrow \infty$, where the implicit constant is absolute.*

We believe that Theorems 3 and 4 in conjunction with Theorem 1 lend credence to Stewart's conjecture when the degree $d \geq 5$. For these degrees, any primitive solutions to (1) either give exceptionally good rational approximations to the lines where the form F vanishes or arise from lattices with exceptionally small first minima. Therefore the existence of any primitive solutions to (1) is indeed exceptional, at least for m large enough.

LATTICES ARISING FROM THUE EQUATIONS

Our goal in this section is to prove Theorem 1. For any form $F(X, Y) \in \mathbb{Z}[X, Y]$ we write \mathbf{F} for the coefficient vector. We first note that $(x, y) \in \mathbb{Q}^2$ is a primitive integral point only if $\|(x, y)\|_p \leq 1$ for all primes p , where $\|\cdot\|_p$ denotes the supnorm. Also, given any positive integer m' , $m'|F(x, y)$ if and only if $|F(x, y)|_p \leq |m'|_p$ for all primes p . We will use the following non-archimedean version

of [9, Lemma 4].

Lemma 1. *Let K be a topologically complete field with respect to a non-archimedean absolute value $|\cdot|$ and $L_1(\mathbf{X}), \dots, L_n(\mathbf{X}) \in K[\mathbf{X}]$ be n linearly independent linear forms. Let $\|\cdot\|$ denote the supnorm on K^n . Suppose $\mathbf{x} \in K^n$ and j is such that*

$$\frac{|L_j(\mathbf{x})|}{\|\mathbf{L}_j\|} \geq \frac{|L_i(\mathbf{x})|}{\|\mathbf{L}_i\|}$$

for $i = 1, \dots, n$. Then

$$\frac{|L_j(\mathbf{x})|}{\|\mathbf{L}_j\|} \geq \frac{\|\mathbf{x}\| |\det(\mathbf{L}_1^{tr}, \dots, \mathbf{L}_n^{tr})|}{\prod_{i=1}^n \|\mathbf{L}_i\|}.$$

Proof. The statement is obvious if $\mathbf{x} = \mathbf{0}$, so suppose otherwise. Then without loss of generality we may assume $\|\mathbf{L}_i\| = 1$ for all i and $\|\mathbf{x}\| = 1$. Let T denote the $n \times n$ matrix with rows \mathbf{L}_i and write

$$\begin{aligned} \mathfrak{m} &= \min_{\substack{\mathbf{y} \in K^n \\ \|\mathbf{y}\|=1}} \{\|T\mathbf{y}^{tr}\|\} \\ \mathfrak{M} &= \max_{\substack{\mathbf{y} \in K^n \\ \|\mathbf{y}\|=1}} \{\|T\mathbf{y}^{tr}\|\}. \end{aligned}$$

Suppose $\|T\mathbf{x}_1^{tr}\| = \mathfrak{m}$ and $\|\mathbf{x}_1\| = 1$. Choose $\mathbf{x}_2, \dots, \mathbf{x}_n \in K^n$, all of length 1, that also satisfy $|\det(\mathbf{x}_1^{tr}, \dots, \mathbf{x}_n^{tr})| = 1$. We then have

$$\begin{aligned} |\det(T)| &= |\det(T)| |\det(\mathbf{x}_1^{tr}, \dots, \mathbf{x}_n^{tr})| = |\det(T\mathbf{x}_1^{tr}, \dots, T\mathbf{x}_n^{tr})| \\ &\leq \prod_{l=1}^n \|T\mathbf{x}_l^{tr}\| \\ &\leq \mathfrak{m} \mathfrak{M}^{n-1}. \end{aligned}$$

Since $\|\mathbf{L}_i\| = 1$ for all i and the absolute value is non-archimedean we have $\mathfrak{M} \leq 1$, so that $\mathfrak{m} \geq |\det(T)|$. On the other hand, by our choice of j we also have $|L_j(\mathbf{x})| \geq |L_i(\mathbf{x})|$ for all $i = 1, \dots, n$. Since $\|\cdot\|$ is the supnorm, these n inequalities (and the definition of T) imply that $|L_j(\mathbf{x})| \geq \|T\mathbf{x}^{tr}\| \geq \mathfrak{m}$. Thus

$$|L_j(\mathbf{x})| \geq \mathfrak{m} \geq |\det(T)| = |\det(\mathbf{L}_1^{tr}, \dots, \mathbf{L}_n^{tr})|.$$

Lemma 2. *Let $F(X, Y) \in \mathbb{Z}[X, Y]$ be a homogeneous polynomial with non-zero discriminant and content 1. Then for every primitive $(x, y) \in \mathbb{Z}^2$ and every prime p with $|F(x, y)|_p < |D(F)|_p$ there is a linear factor $L_p(X, Y) \in \mathbb{Z}_p[X, Y]$ of F with $\|\mathbf{L}_p\|_p = 1$ and*

$$|L_p(x, y)|_p \leq |F(x, y)|_p,$$

with equality if $p \nmid D(F)$.

Proof. Write

$$F(X, Y) = \prod_{i=1}^d M_i(X, Y),$$

where $M_i(X, Y) \in \overline{\mathbb{Q}_p}[X, Y]$ is a linear form for all $i = 1, \dots, d$. Let $|\cdot|_p$ be an absolute value on $\overline{\mathbb{Q}_p}$ that extends the usual p -adic absolute value on \mathbb{Q}_p . Suppose $(x, y) \in \mathbb{Z}^2$ is a primitive integral point and choose i_0 such that

$$\frac{|M_{i_0}(x, y)|_p}{\|\mathbf{M}_{i_0}\|_p} = \min_{1 \leq i \leq d} \left\{ \frac{|M_i(x, y)|_p}{\|\mathbf{M}_i\|_p} \right\}.$$

We note by Lemma 1 that

$$\frac{|M_i(x, y)|_p}{\|\mathbf{M}_i\|_p} \geq \frac{|\det(\mathbf{M}_{i_0}^{tr}, \mathbf{M}_i^{tr})|_p}{\|\mathbf{M}_{i_0}\|_p \|\mathbf{M}_i\|_p} \quad (2)$$

for all $i \neq i_0$, since $\|(x, y)\|_p = 1$.

We claim that M_{i_0} is defined over \mathbb{Q}_p . Indeed, if this were not the case, then without loss of generality there would be a σ in the Galois group of $\overline{\mathbb{Q}_p}$ over \mathbb{Q}_p with $\sigma(M_{i_0}) = M_{i_1}$ for some $i_1 \neq i_0$ between 1 and d . We then have $|M_{i_1}(x, y)|_p = |M_{i_0}(x, y)|_p$ and $\|\mathbf{M}_{i_1}\|_p = \|\mathbf{M}_{i_0}\|_p$ (see [1, chap. 2, Theorem 7]), so that by Lemma 1

$$\frac{|M_{i_0}(x, y)|_p}{\|\mathbf{M}_{i_0}\|_p} \geq \frac{|\det(\mathbf{M}_{i_0}^{tr}, \mathbf{M}_{i_1}^{tr})|_p}{\|\mathbf{M}_{i_0}\|_p \|\mathbf{M}_{i_1}\|_p}. \quad (3)$$

Now by (2), (3), Hadamard's inequality and Gauss' lemma

$$\begin{aligned} \frac{|F(x, y)|_p}{\|\mathbf{F}\|_p} &= \frac{|F(x, y)|_p}{\|\mathbf{M}_1\|_p \cdots \|\mathbf{M}_d\|_p} \geq \frac{|\det(\mathbf{M}_{i_1}^{tr}, \mathbf{M}_{i_0}^{tr})|_p}{\|\mathbf{M}_{i_0}\|_p \|\mathbf{M}_{i_1}\|_p} \prod_{i \neq i_0} \frac{|\det(\mathbf{M}_{i_0}^{tr}, \mathbf{M}_i^{tr})|_p}{\|\mathbf{M}_{i_0}\|_p \|\mathbf{M}_i\|_p} \\ &\geq \prod_{i \neq j} \frac{|\det(\mathbf{M}_i^{tr}, \mathbf{M}_j^{tr})|_p}{\|\mathbf{M}_i\|_p \|\mathbf{M}_j\|_p} \\ &= \frac{|D(F)|_p}{\|\mathbf{M}_1\|_p^{2(d-1)} \cdots \|\mathbf{M}_d\|_p^{2(d-1)}} \\ &= \frac{|D(F)|_p}{\|\mathbf{F}\|_p^{2(d-1)}}. \end{aligned}$$

Since the content of F is 1, we get $|F(x, y)|_p \geq |D(F)|_p$ which contradicts our original hypothesis.

Thus M_{i_0} is defined over \mathbb{Q}_p .

Arguing exactly as above, but this time only using (2), we have

$$\frac{|F(x, y)|_p}{\|\mathbf{F}\|_p} \geq \frac{|M_{i_0}(x, y)|_p}{\|\mathbf{M}_{i_0}\|_p} \frac{|D(F)|_p}{\|\mathbf{F}\|_p^{2(d-1)}}.$$

This gives

$$\frac{|M_{i_0}(x, y)|_p}{\|\mathbf{M}_{i_0}\|_p} \leq \frac{|F(x, y)|_p}{|D(F)|_p}.$$

Since M_{i_0} is defined over \mathbb{Q}_p , we let $L_p(X, Y) \in \mathbb{Z}_p[X, Y]$ be a scalar multiple of $M_{i_0}(X, Y)$ with $\|\mathbf{L}_p\|_p = 1$. We note that if $p \nmid D(F)$, then Hadamard's inequality is actually an equality in all of the above and Lemma 1 gives

$$\frac{|M_i(x, y)|_p}{\|\mathbf{M}_i\|_p} = 1$$

for all $i \neq i_0$. Thus

$$|L_p(x, y)|_p = \frac{|M_{i_0}(x, y)|_p}{\|\mathbf{M}_{i_0}\|_p} = |F(x, y)|_p$$

if $p \nmid D(F)$.

Lemma 3. *Suppose p is a prime and $L(X, Y) \in \mathbb{Z}_p[X, Y]$ is a linear form with $\|\mathbf{L}\|_p = 1$. Let α_p denote the Haar measure on \mathbb{Q}_p with $\alpha_p(\mathbb{Z}_p) = 1$. Then for all integers $c \geq 0$ the set*

$$S = \{(x, y) \in \mathbb{Z}_p^2 : |L(x, y)|_p \leq p^{-c}\}$$

is a \mathbb{Z}_p -module with $\alpha_p^2(S) = p^{-c}$, where α_p^2 denotes the product measure on \mathbb{Q}_p^2 .

Proof. Clearly S is a \mathbb{Z}_p -module. Write $L(X, Y) = aX + bY$ and set

$$M(X, Y) = \begin{cases} Y & \text{if } |a|_p = 1, \\ X & \text{if } |a|_p < 1. \end{cases}$$

Note that in the second case here we necessarily have $|b|_p = 1$ since $\|\mathbf{L}\|_p = 1$. In either case we easily have $\|\mathbf{M}\|_p = 1$ and $|\det(\mathbf{L}^{tr}, \mathbf{M}^{tr})|_p = 1$. Now choose $\mathbf{z}_1, \mathbf{z}_2 \in \mathbb{Z}^2$ with

$$|L(\mathbf{z}_1)|_p = |M(\mathbf{z}_2)|_p = 1, \quad L(\mathbf{z}_2) = M(\mathbf{z}_1) = 1.$$

Then

$$\mathbb{Z}_p^2 = \{x\mathbf{z}_1 + y\mathbf{z}_2 : x, y \in \mathbb{Z}_p\}, \quad S = \{x\mathbf{z}_1 + y\mathbf{z}_2 : x, y \in \mathbb{Z}_p, |x|_p \leq p^{-c}\},$$

so that $\alpha_p^2(S) = p^{-c}(\alpha_p(\mathbb{Z}_p))^2 \alpha_p^2(\mathbb{Z}_p^2) = p^{-c}$.

Lemma 4. *Let \mathcal{S} be a finite set of prime numbers and $L_p(X, Y) \in \mathbb{Z}_p[X, Y]$ be a linear form with $\|\mathbf{L}_p\|_p = 1$ for all $p \in \mathcal{S}$. For each $p \in \mathcal{S}$ let a_p be a positive integer and set*

$$S_p = \{(u, v) \in \mathbb{Z}_p^2 : |L_p(u, v)|_p \leq p^{-a_p}\}.$$

Set $S_p = \mathbb{Z}_p^2$ for all primes $p \notin \mathcal{S}$. Then

$$\Lambda = \bigcap_{p \text{ prime}} \mathbb{Q}^2 \cap S_p$$

is a sublattice of \mathbb{Z}^2 with

$$\det(\Lambda) = \prod_{p \in \mathcal{S}} p^{a_p}.$$

Proof. This follows immediately from Lemma 3 and general facts on lattices and \mathbb{Z}_p -modules (see [11, chap. 3], for example).

Proof of Theorem 1. If $(x, y) \in \mathbb{Z}^2$ is a primitive point with $m|F(x, y)$ and p is a prime dividing m , then $|F(x, y)|_p \leq |m|_p < |D(F)|_p$ so by Lemma 2 there is a linear factor $L_p(x, y) \in \mathbb{Z}_p[X, Y]$ of F with $\|\mathbf{L}_p\|_p = 1$ and $|L_p(x, y)|_p \leq |F(x, y)|_p \leq |m|_p$. There are $c_F(p)$ possible linear factors here by definition, whence $c_F(m)$ choices in total when we consider all primes dividing m . Now suppose for each prime $p|m$ we have chosen a linear factor $L_p(X, Y) \in \mathbb{Z}_p[X, Y]$ of F with $\|\mathbf{L}_p\|_p = 1$. Then by Lemma 4 the set of all $(x, y) \in \mathbb{Z}^2$ with $|L_p(x, y)|_p \leq |m|_p$ for all primes $p|m$ is a sublattice of \mathbb{Z}^2 of determinant m .

PROOF OF THEOREM 2

If $F(X, Y)$ is a any form and $\Lambda = \mathbb{Z}\mathbf{z}_1 \oplus \mathbb{Z}\mathbf{z}_2$ is a lattice, then considering solutions $\mathbf{z} \in \Lambda$ to (1') is the same as considering solutions $(x, y) \in \mathbb{Z}^2$ to the inequality $|F_\Lambda(x, y)| \leq m$, where the form $F_\Lambda(X, Y) := F(X\mathbf{z}_1 + Y\mathbf{z}_2)$. The choice of basis is not unique here of course. We may also view $F_\Lambda(X, Y)$ as a composition $F \circ T$, where $T \in \text{GL}_2(\mathbb{R})$ sends the canonical basis of \mathbb{Z}^2 to a basis of Λ . Note that a different choice of basis amounts to multiplying T by an element of $\text{GL}_2(\mathbb{Z})$.

Our proof will involve various heights which we now define. For any form F written as a product of linear forms, $F(X, Y) = \prod_{i=1}^d L_i(X, Y)$, we set

$$\mathcal{H}(F) = \prod_{i=1}^d \|\mathbf{L}_i\|,$$

where $\|\cdot\|$ denotes the usual L_2 norm on \mathbb{C}^2 . We set

$$\mathcal{M}(F) = \min_{T \in \mathrm{GL}_2(\mathbb{Z})} \mathcal{H}(F \circ T) \quad \text{and} \quad \mathfrak{m}(F) = \min_{\substack{T \in \mathrm{GL}_2(\mathbb{R}) \\ |\det(T)|=1}} \mathcal{H}(F \circ T).$$

We remark that in general (see [10, Lemma 1]) for any form F of degree d and any $T \in \mathrm{GL}_2(\mathbb{R})$,

$$\begin{aligned} D(F \circ T) &= D(F) \det(T)^{d(d-1)} \\ \mathfrak{m}(F \circ T) &= \mathfrak{m}(F) |\det(T)|^{d/2} \\ \mathcal{M}(F) &\geq \mathfrak{m}(F) \geq |D(F)|^{1/2(d-1)}. \end{aligned} \tag{4}$$

In particular, we see that $|D(F_\Lambda)|$, $\mathfrak{m}(F_\Lambda)$ and $\mathcal{M}(F_\Lambda)$ are all well-defined (i.e., are independent of the particular choice of basis) and satisfy

$$|D(F_\Lambda)| = |D(F)| \det(\Lambda)^{d/2}, \quad \mathcal{M}(F_\Lambda) \geq \mathfrak{m}(F_\Lambda) = \mathfrak{m}(F) \det(\Lambda)^{d/2}. \tag{4'}$$

For a given positive integer m we set $\mathcal{M}(F_\Lambda, m)$ to be the minimum of $\mathcal{H}(F_\Lambda)$ over all bases $\mathbf{z}_1, \mathbf{z}_2$ of Λ with \mathbf{z}_1 a solution to (1'), assuming such a primitive solution exists.

The main idea for determining solutions to (1') is to say that some linear factor of F must be relatively small for a given solution. For example, suppose we rewrite $F(X, Y) = a \prod_{i=1}^d (X - \alpha_i Y)$. Now if $(x, y) \in \mathbb{Z}^2$ is any solution to (1'), then

$$|\alpha_i - x/y| \leq \frac{d2^{d-1}m\mathcal{H}(F)^{d-2}}{|y|^d|D(F)|^{1/2}} = d2^{d-1}(\mathcal{H}(F)/m)^{d-2} \frac{m^{d-1}}{|D(F)|^{1/2}} \frac{1}{|y|^d} \tag{5}$$

for some index i by [6 chap. 3, Lemmas 3A and 3B]. An alternative to (5) is that any solution \mathbf{x} to (1') satisfies

$$\frac{|L_i(\mathbf{x})L_j(\mathbf{x})|}{|\det(\mathbf{L}_i^{tr}, \mathbf{L}_j^{tr})|} \leq \frac{2^{d-2}m\mathcal{H}(F)^{d-2}}{\|\mathbf{x}\|^{d-2}|D(F)|^{1/2}} = (2\mathcal{H}(F)/m)^{d-2} \frac{m^{d-1}}{|D(F)|^{1/2}} \frac{1}{\|\mathbf{x}\|^{d-2}} \tag{5'}$$

for some indices i and j ; this is [9, Lemma 5] (with the constants made explicit).

Considering either (5) or (5'), one can see that the major goal is to estimate those solutions $\mathbf{x} = (x, y)$ to (1') either with $|y|$ or $\|\mathbf{x}\|$ “small,” so that any remaining “large” solutions are ϵ -exceptional for some $\epsilon > 0$. Such “large” solutions may be dealt with using gap arguments and ultimately a quantitative version of Roth’s theorem.

We will use the following as the main part of our proof of Theorem 2.

Proposition. *Suppose $F(X, Y) \in \mathbb{Z}[X, Y]$ is a form of degree $d \geq 3$ with non-zero discriminant and content 1, m is a positive integer and $\Lambda \subset \mathbb{R}^2$ is a lattice with $\det(\Lambda) = Am^{2/d}/|D(F)|^{1/d(d-1)}$. Then $\mathcal{M}(F_\Lambda, m) \geq A^{d/2}m$ and if $A \geq 5^4$ the number of primitive lattice points that are solutions to (1') is less than*

$$2 + 2d \left(11 + \frac{\log 2^{10} 3^3 5^3}{\log(d-1)} + \frac{\log 2^9 3^3 5^2}{\log(d-5/4)} + \frac{\log \left(\frac{\log m}{\log(\mathcal{M}(F_\Lambda, m)) - \log m} + 2 \right)}{\log(d-1)} \right).$$

The proof of the Proposition will rely on a few lemmas, though we note that the inequalities $\mathcal{M}(F_\Lambda, m) \geq \mathcal{M}(F_\Lambda) \geq A^{d/2}m$ follow directly from the definitions, (4), (4') and the hypotheses. To prove the Proposition we obviously may assume there is a primitive lattice point $\mathbf{z}_0 \in \Lambda$ that is a solution to (1') since otherwise there is nothing to prove. Given this assumption, we choose a basis $\mathbf{z}_0, \mathbf{z}'_0$ of Λ such that \mathbf{z}_0 is a solution to (1') and $\mathcal{M}(F_\Lambda, m) = \mathcal{H}(F_\Lambda)$. We will write

$$F(X, Y) = \prod_{i=1}^d L_i(X, Y), \quad F_\Lambda(X, Y) = \prod_{i=1}^d X L_i(\mathbf{z}_0) + Y L_i(\mathbf{z}'_0) = F(\mathbf{z}_0) \prod_{i=1}^d X + \alpha_i Y,$$

where $\alpha_i = L_i(\mathbf{z}'_0)/L_i(\mathbf{z}_0)$. For notational convenience, in what follows we will denote the quantity $\mathcal{M}(F_\Lambda, m)/m$ by B . The hypothesis that $A \geq 5^4$ is thus equivalent to the assumption that $B \geq 5^{2d}$.

With the above conventions in place, we see by (4') and (5) that for any solution $\mathbf{z} = x\mathbf{z}_0 + y\mathbf{z}'_0 \in \Lambda$ to (1') with $y \neq 0$ there is some index i with

$$\begin{aligned} |\alpha_i - x/y| &\leq \frac{d2^{d-1}m^{d-1}B^{d-2}}{|y|^d|D(F_\Lambda)|^{1/2}} \\ &= \frac{d2^{d-1}m^{d-1}B^{d-2}}{|y|^d|D(F)|^{1/2}\det(\Lambda)^{d(d-1)/2}} \\ &\leq \frac{d2^{d-1}B^{d-2}}{|y|^d(5^4)^{d(d-1)/2}} \\ &< \frac{B^{d-2}}{2|y|^d}. \end{aligned} \tag{6}$$

We may utilize a standard gap principle argument to estimate those solutions with $|y| > B$, for example (see Lemma 7 below). Eventually we come to the point where a quantitative version of Roth's theorem is invoked (Lemma 8). But before we do that, we deal with those solutions where $|y|$ is smaller. The following is a variation on [6, chap. 3, Lemma 5B].

Lemma 5. *For every primitive lattice point $\mathbf{z} = x\mathbf{z}_0 + y\mathbf{z}'_0 \in \Lambda$ with $y \neq 0$ that is a solution to (1'), there are $\psi_1(\mathbf{z}), \dots, \psi_d(\mathbf{z}) \in [0, 1]$ that, if not zero, are at least $1/(2d)$, satisfy $\sum_{i=1}^d \psi_i(\mathbf{z}) \geq 1/2$, and also*

$$\frac{|L_i(\mathbf{z}_0)|}{|L_i(\mathbf{z})|} \geq (B^{\psi_i(\mathbf{z})} - 2)|y|$$

for all $i = 1, \dots, d$.

Proof. We first claim that $2|L_{i_0}(\mathbf{z}_0)| \leq |L_{i_0}(\mathbf{z})|$ for some index i_0 . Indeed, if this were not the case then $\Lambda' := \mathbb{Z}\mathbf{z}_0 \oplus \mathbb{Z}\mathbf{z}$ is a sublattice of Λ and $F_{\Lambda'}(X, Y) := F(X\mathbf{z}_0 + Y\mathbf{z})$ satisfies

$$\mathcal{H}(F_{\Lambda'})^2 = \prod_{i=1}^d |L_i(\mathbf{z}_0)|^2 + |L_i(\mathbf{z})|^2 < \prod_{i=1}^d 5|L_i(\mathbf{z}_0)|^2 \leq 5^d m^2$$

since \mathbf{z}_0 is a solution to (1'). But now by (4), (4') and the hypotheses we have a contradiction:

$$\begin{aligned} 5^{d/2}m &> \mathcal{H}(F_{\Lambda'}) \geq \mathfrak{m}(F) \det(\Lambda')^{d/2} \\ &\geq \mathfrak{m}(F) \det(\Lambda)^{d/2} \\ &\geq |D(F)|^{1/2(d-1)} \det(\Lambda)^{d/2} \\ &\geq 5^{2d}m. \end{aligned}$$

With the claim shown, choose an index i_0 with $2|L_{i_0}(\mathbf{z}_0)| \leq |L_{i_0}(\mathbf{z})|$. Since \mathbf{z} is a primitive lattice point there is a $\mathbf{z}' \in \Lambda$ with $\Lambda = \mathbb{Z}\mathbf{z} \oplus \mathbb{Z}\mathbf{z}'$. Further, we may add any integer multiple of \mathbf{z} to \mathbf{z}' here. Thus, we may choose \mathbf{z}' such that $\alpha := \Re(L_{i_0}(\mathbf{z}')/L_{i_0}(\mathbf{z}))$ satisfies $|\alpha| \leq 1/2$. We now write $\mathbf{z}_0 = z\mathbf{z} + z'\mathbf{z}'$ for some $z, z' \in \mathbb{Z}$ with $|z'| = [\Lambda : \mathbb{Z}\mathbf{z}_0 \oplus \mathbb{Z}\mathbf{z}] = |y|$. For any linear form $L(X, Y)$ we have

$$\frac{L(\mathbf{z}_0)}{L(\mathbf{z})} = z + z' \frac{L(\mathbf{z}')}{L(\mathbf{z})}.$$

In particular, using $L = L_{i_0}$ we see that $|z + z'\alpha| \leq 1/2$, and for all $i = 1, \dots, d$

$$\begin{aligned} \frac{|L_i(\mathbf{z}_0)|}{|L_i(\mathbf{z})|} &= \left| z + z' \frac{L_i(\mathbf{z}')}{L_i(\mathbf{z})} \right| \\ &= \left| z' \left(\frac{L_i(\mathbf{z}')}{L_i(\mathbf{z})} - \alpha \right) + z + z'\alpha \right| \\ &\geq \left| z' \left(\frac{L_i(\mathbf{z}')}{L_i(\mathbf{z})} - \alpha \right) \right| - |z + z'\alpha| \\ &\geq |z'| \left(\left| \frac{L_i(\mathbf{z}')}{L_i(\mathbf{z})} \right| - \frac{1}{2} \right) - \frac{1}{2} \\ &\geq |y| \left(\left| \frac{L_i(\mathbf{z}')}{L_i(\mathbf{z})} \right| + 1 - 2 \right). \end{aligned} \tag{7}$$

Since $|F(\mathbf{z})| \leq m$ and $\Lambda = \mathbb{Z}\mathbf{z} \oplus \mathbb{Z}\mathbf{z}'$,

$$\begin{aligned}
\prod_{i=1}^d \left(1 + \left| \frac{L_i(\mathbf{z}')}{L_i(\mathbf{z})} \right| \right) &\geq \prod_{i=1}^d \sqrt{1 + \left| \frac{L_i(\mathbf{z}')}{L_i(\mathbf{z})} \right|^2} \\
&= \frac{1}{|F(\mathbf{z})|} \prod_{i=1}^d \sqrt{|L_i(\mathbf{z})|^2 + |L_i(\mathbf{z}')|^2} \\
&\geq \frac{\mathcal{M}(F_\Lambda, m)}{|F(\mathbf{z})|} \\
&\geq B.
\end{aligned} \tag{8}$$

We define $\psi_i(\mathbf{z})$ by

$$B^{\psi_i(\mathbf{z})} = \begin{cases} B & \text{if } \left| \frac{L_i(\mathbf{z}')}{L_i(\mathbf{z})} \right| + 1 \geq B, \\ 1 & \text{if } \left| \frac{L_i(\mathbf{z}')}{L_i(\mathbf{z})} \right| + 1 < B^{1/(2d)}, \\ \left| \frac{L_i(\mathbf{z}')}{L_i(\mathbf{z})} \right| + 1 & \text{otherwise.} \end{cases}$$

Now by construction $0 \leq \psi_i(\mathbf{z}) \leq 1$ for all $i = 1, \dots, d$ and any $\psi_j(\mathbf{z}) \geq 1/2d$ if it isn't zero. We have $\sum_{i=1}^d \psi_i(\mathbf{z}) \geq 1$ if any $\psi_j(\mathbf{z}) = 1$, so suppose $\psi_i(\mathbf{z}) < 1$ for all $i = 1, \dots, d$. Then by (8)

$$\begin{aligned}
B^{1/2} \prod_{i=1}^d B^{\psi_i(\mathbf{z})} &> \prod_{\substack{1 \leq i \leq d \\ \psi_i(\mathbf{z})=0}} \left(1 + \left| \frac{L_i(\mathbf{z}')}{L_i(\mathbf{z})} \right| \right) \prod_{\substack{1 \leq i \leq d \\ \psi_i(\mathbf{z})>0}} B^{\psi_i(\mathbf{z})} \\
&= \prod_{1 \leq i \leq d} \left(1 + \left| \frac{L_i(\mathbf{z}')}{L_i(\mathbf{z})} \right| \right) \\
&\geq B.
\end{aligned}$$

This shows that $\sum_{i=1}^d \psi_i(\mathbf{z}) \geq 1/2$ in all cases. Also by construction $B^{\psi_i(\mathbf{z})} \leq \left| \frac{L_i(\mathbf{z}')}{L_i(\mathbf{z})} \right| + 1$ for all i , so that the remaining desired inequalities follow from (7).

Lemma 6. *For all $c > 0$ there are less than $2d(2c + 1)$ primitive solutions $\mathbf{z} = x\mathbf{z}_0 + y\mathbf{z}'_0 \in \Lambda$ to (1') with $y \neq 0$ and $|y| \leq B^c$.*

We thus are able to rather efficiently estimate solutions where $|y| \leq B^c$ for any fixed constant c . In particular, though it's certainly possible to improve upon particular aspects of Lemma 5, there wouldn't be much to gain (the exception being if one could improve upon B , specifically, if one could replace B by a larger quantity in terms of m or F). However, we remark that the hypothesis $\det(\Lambda) \geq 5^4 m^{2/d} |D(F)|^{1/d(d-1)}$ can be relaxed to $\det(\Lambda) \geq 5^4 (m/\mathfrak{m}(F))^{2/d}$, both in Lemma 5 and here in Lemma 6.

Proof. By Lemma 5

$$\frac{|L_i(\mathbf{z})|}{|L_i(\mathbf{z}_0)|} = |\alpha_i - x/y| \leq \frac{1}{(B^{\psi_i(\mathbf{z})} - 2)|y|^2} \quad (9)$$

for all solutions $\mathbf{z} = x\mathbf{z}_0 + y\mathbf{z}'_0 \in \Lambda$ to (1') with $y \neq 0$ and all $i = 1, \dots, d$.

Let \mathcal{S} denote the set of primitive solutions $\mathbf{z} = x\mathbf{z}_0 + x\mathbf{z}'_0 \in \Lambda$ to (1') with $1 \leq y \leq B^c$. For the moment fix an index i and consider the sum $\sum \psi_i(\mathbf{z})$ over all $\mathbf{z} \in \mathcal{S}$. Obviously we may restrict to solutions with $\psi_i(\mathbf{z}) \neq 0$; we arrange these solutions $\mathbf{z}_l = x_l\mathbf{z}_0 + y_l\mathbf{z}'_0$, $l = 1, \dots, n$ so that $y_l \leq y_{l+1}$ for all l . Then by Lemma 5 and (9)

$$\begin{aligned} \frac{1}{|y_l y_{l+1}|} &\leq \left| \frac{x_l}{y_l} - \frac{x_{l+1}}{y_{l+1}} \right| \\ &\leq \left| \alpha_i - \frac{x_l}{y_l} \right| + \left| \alpha_i - \frac{x_{l+1}}{y_{l+1}} \right| \\ &\leq \frac{1}{(B^{\psi_i(\mathbf{z}_l)} - 2)|y_l|^2} + \frac{1}{(B^{\psi_i(\mathbf{z}_{l+1})} - 2)|y_{l+1}|^2} \\ &\leq \frac{1}{(B^{\psi_i(\mathbf{z}_l)} - 2)|y_l|^2} + \frac{1}{(B^{\psi_i(\mathbf{z}_{l+1})} - 2)|y_l y_{l+1}|}, \end{aligned}$$

whence

$$|y_{l+1}| \geq (B^{\psi_i(\mathbf{z}_l)} - 2)(1 - (B^{\psi_i(\mathbf{z}_{l+1})} - 2)^{-1})|y_l|. \quad (10)$$

Since $\psi_i(\mathbf{z}_l) \geq 1/2d$ for all our \mathbf{z}_l and $B \geq 5^{2d}$, we have $B^{\psi_i(\mathbf{z}_l)} \geq 5$ and thus $B^{\psi_i(\mathbf{z}_l)} - 3 \geq B^{\psi_i(\mathbf{z}_l) \log 2 / \log 5}$. We now repeatedly apply (10) to get

$$\begin{aligned} B^c \geq |y_n| &\geq (B^{\psi_i(\mathbf{z}_1)} - 2)(B^{\psi_i(\mathbf{z}_2)} - 3) \dots (B^{\psi_i(\mathbf{z}_{n-1})} - 3)(1 - (B^{\psi_i(\mathbf{z}_n)} - 2)^{-1})|y_1| \\ &> \prod_{l=1}^{n-1} (B^{\psi_i(\mathbf{z}_l)} - 3) \times (1 - (1/3)) \\ &\geq (2/3) \prod_{l=1}^{n-1} B^{\psi_i(\mathbf{z}_l) \log 2 / \log 5}. \end{aligned}$$

Taking logarithms yields

$$c + \log_B(3/2) > \sum_{l=1}^{n-1} \psi_i(\mathbf{z}_l) \log 2 / \log 5,$$

and since $\psi_i(\mathbf{z}_n) \leq 1$,

$$c + \log_B(3/2) + \log 2 / \log 5 > \sum_{l=1}^n \psi_i(\mathbf{z}_l) \log 2 / \log 5 = \sum_{\mathbf{z} \in \mathcal{S}} \psi_i(\mathbf{z}) \log 2 / \log 5.$$

Finally, by Lemma 5 and this last inequality

$$\begin{aligned}
|\mathcal{S}| &\leq \sum_{\mathbf{z} \in \mathcal{S}} \sum_{i=1}^d 2\psi_i(\mathbf{z}) \\
&= \sum_{i=1}^d \sum_{\mathbf{z} \in \mathcal{S}} 2\psi_i(\mathbf{z}) \\
&< \sum_{i=1}^d 2c + 2\log_B(3/2) + 2\log 2/\log 5 \\
&\leq \sum_{i=1}^d 2c + 2\log(3/2)/\log(5^{2d}) + 2\log 2/\log 5 \\
&= \sum_{i=1}^d 2c + \log(3/2)/d\log 5 + 2\log 2/\log 5 \\
&\leq \sum_{i=1}^d 2c + \log(3/2)/3\log 5 + 2\log 2/\log 5 \\
&< d(2c + 1).
\end{aligned}$$

The same argument works for estimating the number of primitive solutions $x\mathbf{z}_0 + y\mathbf{z}'_0$ to (1') with $1 \leq -y \leq B^c$.

Lemma 7. *For all $C_2 > C_1 > B$, the number of primitive solutions $\mathbf{z} = x\mathbf{z}_0 + y\mathbf{z}'_0 \in \Lambda$ to (1') with $C_1 \leq |y| \leq C_2$ is less than*

$$2d \left(1 + \frac{\log(\log C_2 / \log(C_1/B))}{\log(d-1)} \right).$$

Proof. We will use (6). Suppose $x\mathbf{z}_0 + y\mathbf{z}'_0, x'\mathbf{z}_0 + y'\mathbf{z}'_0 \in \Lambda$ are primitive solutions to (1') with both

$$|\alpha_i - x/y| < \frac{B^{d-2}}{2|y|^d}, \quad |\alpha_i - x'/y'| < \frac{B^{d-2}}{2|y'|^d}$$

for some index i . Suppose further that $y' \geq y > 0$. Then by the inequalities above

$$\begin{aligned}
\frac{1}{|yy'|} &\leq \left| \frac{x}{y} - \frac{x'}{y'} \right| \\
&\leq \left| \alpha_i - \frac{x}{y} \right| + \left| \alpha_i - \frac{x'}{y'} \right| \\
&< \frac{B^{d-2}}{2|y|^d} + \frac{B^{d-2}}{2|y'|^d} \\
&\leq \frac{B^{d-2}}{|y|^d},
\end{aligned}$$

so that $|y'| \geq |y|^{d-1}/B^{d-2}$. Hence if $x_1\mathbf{z}_0 + y_1\mathbf{z}'_0, x_2\mathbf{z}_0 + y_2\mathbf{z}'_0, \dots$ are primitive solutions to (1') as above with $C_1 \leq y_1 \leq y_2 \leq \dots \leq C_2$, then repeatedly applying the above inequality yields

$$C_2 \geq y_{l+1} \geq \frac{y_1^{(d-1)^l}}{B^{((d-1)^{l-1} + \dots + 1)(d-2)}} \geq \frac{C_1^{(d-1)^l}}{B^{(d-1)^l - 1}} > (C_1/B)^{(d-1)^l}$$

for all $l \geq 1$. We take logarithms twice to get

$$\frac{\log(\log C_2 / (\log C_1 / B))}{\log(d-1)} > l.$$

Taking into account the d possible indices i and employing the same argument for solutions with $y < 0$ gives the lemma.

Lemma 8. *Then there are less than*

$$2d \left(4 + \frac{\log 2^9 3^3 5^2}{\log(d-5/4)} \right)$$

primitive $\mathbf{z} = x\mathbf{z}_0 + \mathbf{z}'_0 \in \Lambda$ solutions to (1') with $|y| \geq \max\{B^{4(d-1)}, (8^d \mathcal{M}(F_\Lambda, m))^{2^{10} 3^3 5^3}\}$.

Proof. We note that the α_i are conjugate algebraic numbers with absolute height

$$h(\alpha_i)^d = \mathcal{H}(F_\Lambda) = \mathcal{M}(F_\Lambda, m)$$

(see [6, chap. 3, Lemma 2A], for example). Given a solution as in the lemma, by (10) and the hypothesis $|y| \geq B^{4(d-1)}$ we have

$$\begin{aligned} |\alpha_i - x/y| &\leq \frac{d2^{d-1}B^{d-2}}{|y|^d} \\ &< \frac{B^{d-1}}{2|y|^d} \\ &\leq \frac{1}{2|y|^{d-1/4}} \end{aligned} \tag{11}$$

for some index i . We claim that

$$|\alpha_i - x/y| < (H(x/y))^{-\sqrt{2d}(1+1/20)}, \tag{12}$$

where $H(x/y) = \sqrt{x^2 + y^2}$ is the (absolute) height of x/y . To see this, we first note that $|x/y| < |\alpha_i| + 1$, so that $H(x/y) < (|\alpha_i| + 2)|y| \leq 3h(\alpha_i)^d|y|$. Since $d \geq 3$, one readily verifies that

$d - 1/4 \geq \sqrt{2d}(1 + 1/10)$. Using this we easily get $(3h(\alpha_i)^d)^{d-1/4} < (3h(\alpha_i)^d)^{\sqrt{d}} < y^{\sqrt{2d}/20}$ (with quite a bit of room to spare, in fact). In addition, we also get

$$\begin{aligned} y^{d-1/4} &\geq \left(\frac{H(x/y)}{3h(\alpha_i)^d} \right)^{d-1/4} \\ &> H(x/y)^{\sqrt{2d}(1+1/10)} y^{-\sqrt{2d}/20} \\ &\geq H(x/y)^{\sqrt{2d}(1+1/10)} H(x/y)^{-\sqrt{2d}/20} \\ &= H(x/y)^{\sqrt{2d}(1+1/20)}. \end{aligned}$$

Therefore, (12) follows from (11).

According to [6, chap. 2, Theorem 6] (with $m = 2$ and $\chi = 1/20$ there), the rational solutions x/y to (12) satisfy $H(x/y) \leq (8h(\alpha_i))^{d2^{10}3^35^3}$ or $w \leq H(x/y) < w^{2^93^35^2d^2}$ for some $w > 1$. The first option here is ruled out for us by hypothesis since $H(x/y) \geq |y|$. Hence it remains to estimate the number of primitive solutions (x, y) to (11) with $w/(3h(\alpha_i)^d) \leq |y| < w^{2^93^35^2d^2}$. We clearly may assume that $w \geq (8h(\alpha_i))^{4d}$.

Suppose $(x_0, y_0), (x_1, y_1), \dots$ are the primitive solutions to (11) with $y_i > 0$ and arranged so that $0 < y_0 \leq y_1 \leq \dots$. We then have

$$\begin{aligned} \frac{1}{|y_l y_{l+1}|} &\leq \left| \frac{x_l}{y_l} - \frac{x_{l+1}}{y_{l+1}} \right| \\ &\leq \left| \alpha_i - \frac{x_l}{y_l} \right| + \left| \alpha_i - \frac{x_{l+1}}{y_{l+1}} \right| \\ &< \frac{1}{2|y_l|^{d-1/4}} + \frac{1}{2|y_{l+1}|^{d-1/4}} \\ &\leq \frac{1}{|y_l|^{d-1/4}}, \end{aligned}$$

so that $|y_{l+1}| \geq |y_l|^{d-5/4}$ for all $l \geq 0$. Moreover, since $w \geq (8^d h(\alpha_i)^d)^4$ and $d \geq 3$ we have

$$w^{d-2} \geq (8h(\alpha_i))^{4d} > (3h(\alpha_i)^d)^{2(d-2)} B^{2(d-2)} \geq (3h(\alpha_i)^d B)^{d-1},$$

so that also by (11)

$$y_1 \geq \frac{y_0^{d-1}}{B^{d-1}} \geq \left(\frac{w}{3h(\alpha_i)^d B} \right)^{d-1} > \frac{w^{d-1}}{w^{d-2}} = w.$$

We thus have $y_l \geq w^{(d-5/4)^l}$ for all $l \geq 1$. Now since all $y_l < w^{2^93^35^2d^2}$, we must have

$$l < \frac{\log 2^93^35^2d^2}{\log(d-5/4)} < 3 + \frac{\log 2^93^35^2}{\log(d-5/4)}.$$

Considering the d possible indices i above and accounting for those solutions with $y < 0$ in the same manner completes the proof.

Proof of the Proposition. We first set $c = 2$ in Lemma 6 to see that the number of primitive solutions $\mathbf{z} = x\mathbf{z}_0 + y\mathbf{z}'_0 \in \Lambda$ to (1') with $1 \leq |y| \leq B^2$ is less than $10d$. Next we set $C_1 = B^2$ and $C_2 = B^{4(d-1)}$ in Lemma 7 to see that the number of solutions with $B^2 \leq |y| \leq B^{4(d-1)}$ is less than

$$2d \left(1 + \frac{\log(\log B^{4(d-1)} / \log B)}{\log(d-1)} \right) = 2d(2 + \log 4 / \log(d-1)).$$

If on the other hand we set $C_2 = (8^d \mathcal{M}(F_\Lambda, m))^{2^{10}3^35^3}$, then (recall $B \geq 5^{2d} > 8^d$) the number of solutions with $B^2 \leq |y| \leq (8^d \mathcal{M}(F_\Lambda, m))^{2^{10}3^35^3}$ is less than

$$\begin{aligned} 2d \left(1 + \frac{\log(2^{10}3^35^3 \log(8^d \mathcal{M}(F_\Lambda, m)) / \log B)}{\log(d-1)} \right) \\ < 2d \left(1 + \frac{\log(2^{10}3^35^3(1 + \log(\mathcal{M}(F_\Lambda, m)) / \log B))}{\log(d-1)} \right) \\ = 2d \left(1 + \frac{\log(2^{10}3^35^3(2 + \log m / \log B))}{\log(d-1)} \right) \\ = 2d \left(1 + \frac{\log 2^{10}3^35^3}{\log(d-1)} + \frac{\log(2 + \log m / \log B)}{\log(d-1)} \right). \end{aligned}$$

Therefore the number of solutions with $B^2 \leq |y| \leq \max\{B^{4(d-1)}, (8^d \mathcal{M}(F_\Lambda, m))^{2^{10}3^35^3}\}$ is less than

$$2d \left(2 + \frac{\log 2^{10}3^35^3}{\log(d-1)} + \frac{\log(2 + \log m / \log B)}{\log(d-1)} \right).$$

Combining this with Lemma 8, the number of solutions with $y \neq 0$ is less than

$$10d + 2d \left(6 + \frac{\log 2^{10}3^35^3}{\log(d-1)} + \frac{\log 2^93^35^2}{\log(d-5/4)} + \frac{\log(2 + \log m / \log B)}{\log(d-1)} \right).$$

Of course, we also have the two solutions $\pm \mathbf{z}_0$ as well, giving the Proposition.

Proof of Theorem 2. Suppose first that $A \geq 5^4$. We may assume that there is a primitive solution $(x, y) \in \Lambda$ to (1'). We apply the Proposition, noting that

$$\log(\mathcal{M}(F_\Lambda, m)/m) \geq \log(A^{d/2}), \quad \frac{\log(2^{10}3^35^3)}{\log(d-1)} + \frac{\log(2^93^35^2)}{\log(d-5/4)} < \frac{31}{\log(d-1)}$$

since $d \geq 3$. For $A < 5^4$ we use the Proposition in conjunction with Lemma 2C (and Remark 2D) of [6, chap. 3] as follows. Let p be any prime satisfying $(5^4/A) \leq p \leq 2(5^4/A) - 1$ and let F be a form as in the Proposition except that $A < 5^4$. Then there are $p+1$ forms G with $|D(G)| = |D(F)|p^{d(d-1)}$ and any primitive integer solution (x, y) to (1') is a primitive integral solution to $|G(x, y)| \leq m$ for one of these forms G . Since

$$\det(\Lambda) = \frac{Am^{2/d}}{|D(F)|^{1/d(d-1)}} = \frac{Am^{2/d}p}{|D(G)|^{1/d(d-1)}} \geq \frac{5^4m^{2/d}}{|D(G)|^{1/d(d-1)}},$$

we may apply the Proposition to these $p+1 \leq 2(5^4/A)$ forms G to prove the case of Theorem 2 when $A < 5^4$.

PROOF OF THEOREMS 3 AND 4

Proof of Theorem 3. Let $\Lambda \subseteq \mathbb{Z}^2$ be a sublattice with $\det(\Lambda) = m(F)$. Denote the successive minima of Λ (with respect to the unit disk) by $\lambda_1 \leq \lambda_2$. By Minkowski's theorem,

$$\lambda_2^2 \geq \lambda_1 \lambda_2 \geq (2^2/2!) \frac{\det(\Lambda)}{\pi} = \frac{2m(F)}{\pi}. \quad (13)$$

We clearly have $m(F) \geq m/|D(F)|$. Thus for m sufficiently large (depending on both F and ϵ),

$$m(F)^{1+\epsilon/12} > m, \quad m(F)^{\epsilon/12} \geq \frac{2^{d-2}\mathcal{H}(F)^{d-2}}{(2/\pi)^{1+\epsilon/2}|D(F)|^{1/2}}. \quad (14)$$

Now suppose $\mathbf{x} = (x, y) \in \Lambda$ is a primitive lattice point with $\|(x, y)\| \geq \lambda_2$. If (x, y) is a solution to (1'), then by (5'), (13) and (14) there are indices $i \neq j$ with

$$\begin{aligned} \frac{|L_i(\mathbf{x})L_j(\mathbf{x})|}{|\det(\mathbf{L}_i^{tr}, \mathbf{L}_j^{tr})|} &\leq \frac{2^{d-2}m\mathcal{H}(F)^{d-2}}{\|\mathbf{x}\|^{d-2}|D(F)|^{1/2}} \\ &\leq \frac{2^{d-2}m\mathcal{H}(F)^{d-2}}{\lambda_2^{2+\epsilon}\|\mathbf{x}\|^{d-4-\epsilon}|D(F)|^{1/2}} \\ &\leq \frac{2^{d-2}m\mathcal{H}(F)^{d-2}}{m(F)^{1+\epsilon/2}(2/\pi)^{1+\epsilon/2}\|\mathbf{x}\|^{d-4-\epsilon}|D(F)|^{1/2}} \\ &= \frac{m}{m(F)^{1+\epsilon/4}} \frac{2^{d-2}\mathcal{H}(F)^{d-2}}{m(F)^{\epsilon/4}(2/\pi)^{1+\epsilon/2}|D(F)|^{1/2}} \frac{1}{\|\mathbf{x}\|^{d-4-\epsilon}} \\ &< \frac{1}{\|\mathbf{x}\|^{d-4-\epsilon}}. \end{aligned}$$

Thus $\mathbf{x} = (x, y)$ is $(d-4-\epsilon)$ -exceptional. For notational convenience temporarily set $\delta = \epsilon/3(2+\epsilon)$.

Now if $\mathbf{x} = (x, y) \in \Lambda$ is a primitive solution to (1') with $\|\mathbf{x}\| = \lambda_1$ and $\lambda_1 \geq m(F)^{(1/2)-\delta}$, then as

above (this time using the full strength of (14)) there are indices $i \neq j$ with

$$\begin{aligned}
\frac{|L_i(\mathbf{x})L_j(\mathbf{x})|}{|\det(\mathbf{L}_i^{tr}, \mathbf{L}_j^{tr})|} &\leq \frac{2^{d-2}m\mathcal{H}(F)^{d-2}}{\|\mathbf{x}\|^{d-2}|D(F)|^{1/2}} \\
&= \frac{2^{d-2}m\mathcal{H}(F)^{d-2}}{\lambda_1^{2+\epsilon}\|\mathbf{x}\|^{d-4-\epsilon}|D(F)|^{1/2}} \\
&< \frac{2^{d-2}m\mathcal{H}(F)^{d-2}}{m(F)^{((1/2)-\delta)(2+\epsilon)}\|\mathbf{x}\|^{d-4-\epsilon}|D(F)|^{1/2}} \\
&= \frac{2^{d-2}m\mathcal{H}(F)^{d-2}}{m(F)^{1+\epsilon/6}\|\mathbf{x}\|^{d-4-\epsilon}|D(F)|^{1/2}} \\
&= \frac{m}{m(F)^{1+\epsilon/12}} \frac{2^{d-2}\mathcal{H}(F)^{d-2}}{m(F)^{\epsilon/12}|D(F)|^{1/2}} \frac{1}{\|\mathbf{x}\|^{d-4-\epsilon}} \\
&< \frac{1}{\|\mathbf{x}\|^{d-4-\epsilon}}.
\end{aligned}$$

Thus \mathbf{x} is again $(d-4-\epsilon)$ -exceptional. This shows that any primitive solution $\mathbf{x} = (x, y) \in \Lambda$ to (1') that is not $(d-4-\epsilon)$ -exceptional must satisfy $\lambda_2 > \|\mathbf{x}\| = \lambda_1 < m(F)^{(1/2)-\delta}$. There can be at most one pair $\pm(x, y)$ of such primitive lattice points by the definition of successive minima.

Proof of Theorem 4. The number of sublattices $\Lambda \subseteq \mathbb{Z}^2$ with determinant m is equal to $\sum_{n|m} n$ (see [5, §3], for example), thus the number N of such lattices satisfies $m \leq N \ll m \log \log m$ (though we will only use the lower bound here). On the other hand, any primitive $(x, y) \in \mathbb{Z}^2$ is a lattice point in exactly one sublattice $\Lambda \subseteq \mathbb{Z}^2$ with $m = \det(\Lambda) > (\pi/2)\|(x, y)\|^2$. Indeed, for such a lattice we must have $\|(x, y)\| = \lambda_1 < \lambda_2$ by (13), so that $\Lambda = \mathbb{Z}(x, y) \oplus \mathbb{Z}(x', y')$ for some $(x', y') \in \mathbb{Z}^2$ with $xy' - x'y = m$. Since (x, y) is a primitive point, there is an $(x', y') \in \mathbb{Z}^2$ with $xy' - x'y = m$. Moreover, from elementary number theory any other such point is of the form $(x', y') + n(x, y)$ for some integer n . Hence any sublattice of determinant m containing (x, y) has the same basis, so there is only one such sublattice.

Now suppose $\delta > 0$. If $m^{2\delta} < \pi/2$ then there is nothing to prove since $O(m^{-2\delta}) = O(1)$. Otherwise we have $(\pi/2)m^{1-2\delta} \leq m$. By what we have shown, the number of sublattices $\Lambda \subseteq \mathbb{Z}^2$ with $\det(\Lambda) = m$ that contain a primitive (x, y) with $\|(x, y)\| \leq m^{(1/2)-\delta}$ is equal to the number N' of such primitive points. Clearly N' is no greater than the total number of integral points in the disk with radius $m^{(1/2)-\delta}$, which in turn is no greater than $4\pi m^{1-2\delta}$. (The number of integral points in the disk of radius $r \geq 1$ is no more than $\pi(r+1)^2 \leq 4\pi r^2$.) Thus $N' \leq 4\pi m^{1-2\delta}$ and so the proportion of such lattices $N'/N = O(m^{-2\delta})$.

REFERENCES

- [1] E. Artin, *Algebraic Numbers and Algebraic Functions*, Gordon and Breach, Basel, 1967.
- [2] E. Bombieri and W.M. Schmidt, *On Thue's equation*, Inv. Math. **88** (1987), 69–81.
- [3] J.-H. Evertse, *On equations in S -units and the Thue-Mahler equation*, Invent. Math. **75** (1984), 561–584.
- [4] D.J. Lewis and K. Mahler, *On the representation of integers by binary forms*, Acta Arith. **6** (1961), 333–363.
- [5] W.M. Schmidt, *Asymptotic formulæ for point lattices of bounded determinant and subspaces of bounded height*, Duke Math. J. **35** (1968), 327–339.
- [6] ———, *Diophantine approximation*, Springer Lecture Notes in Mathematics 1467, Springer-Verlag, New York, 1991.
- [7] C. Stewart, *On the number of solutions of polynomial congruences and Thue equations*, Jour. Amer. Math. Soc. **4** (1991), 793–835.
- [8] A. Thue, *Über Annäherungswerte algebraischer Zahlen*, J. Reine Angew. Math. **135** (1909), 284–305.
- [9] J.L. Thunder, *Decomposable form inequalities*, Ann. Math. **153** (2001), 767–804.
- [10] ———, *Asymptotic estimates for the number of integer solutions to decomposable form inequalities*, Comp. Math. **141** (2005), 271–292.
- [11] A. Weil, *Basic Number Theory*, Springer-Verlag, New York, 1974.

DEPARTMENT OF MATHEMATICS, NORTHERN ILLINOIS UNIVERSITY, DEKALB, IL 60115
E-mail address: `jthunder@math.niu.edu`